A Deep Learning Approach to Cybersecurity Chatbots: Combining BERT, Cosine Similarity, and Natural Language Processing

Amit Nagal
TCPWave Pvt. Limited, India

Murali Sappa
TCPWave Pvt. Limited, India

ABSTRACT

This study evaluates the comparative performance of Logistic Regression, Naive Bayes, and Support Vector Machines against the paraphrase-distilroberta-base-v1 deep learning model. By encoding textual data into 768 dimensional vector embeddings, the research optimizes semantic search and clustering within complex network environments. The investigation meticulously assesses the "Alice" chatbot, leveraging natural language processing and cosine similarity to navigate intricate frameworks and provide rapid, accurate responses. Crucially, the article examines Alice's efficacy in detecting adversarial attacks and augmenting Security Information and Event Management (SIEM) systems. By analyzing the impact of NLP-driven agents on network monitoring, this research elucidates how such technologies bolster operational efficiency and user engagement. Ultimately, these findings underscore the critical integration of AI-driven chatbots in fortifying defensive postures and streamlining workflows within the cybersecurity and network security sectors.

INTRODUCTION

Traditional NLP algorithms have limited functionality. The present papers explain how Sentence transformer models, a sub-type of Large Language Models (LLMs), are designed to embed sentences and text passages into high-dimensional vector spaces. This approach captures the semantic relationships between sentences by encoding them as vectors, enabling a more nuanced representation of textual data.

DOI: 10.4018/407631

In contrast to traditional word embedding methods that focus on individual words, sentence transformers consider the holistic meaning of the entire sentence during the embedding process.

The present study delves into the multifaceted capabilities of an innovative chatbot Alice, designed to revolutionize user interactions by integrating cutting-edge Natural Language Processing (NLP) techniques. Alice serves as a virtual assistant adept at handling inquiries about Network Management. Through its seamless integration within the Network ecosystem, Alice aims to streamline user experiences by providing swift resolutions to queries and executing tasks efficiently. By harnessing the power of NLP using DistilRoBERTa-based, Alice comprehends user inputs and adapts to evolving conversational contexts, enhancing overall customer satisfaction. The growing demand for customer service chatbots is gaining popularity across industries like cybersecurity and network management rasa.

OBJECTIVES OF STUDY

1. To evaluate the effectiveness of deep learning models compared to traditional machine learning approaches in chatbot development.
2. To analyze the role of sentence transformers and cosine similarity in enhancing semantic understanding.
3. To compare frameworks such as RASA, Chatterbot, and custom-trained models for cybersecurity applications.
4. To identify limitations of current chatbot architectures and propose future research directions.

LITERATURE REVIEW

Gayathri et al. (2022) demonstrated that BERT-based transformer models could effectively identify suicidal ideation in tweets, offering a high-accuracy technical approach to mental health monitoring on social media. This work highlighted the broader potential of transformer-based architectures in sensitive domains, setting the stage for their adoption in cybersecurity and network management.

Building on this, Bocklisch et al. (2017) introduced Rasa, an influential open-source framework that decoupled dialogue management from natural language understanding. By enabling developers to build flexible, non-linear conversational AI, Rasa became a cornerstone for scalable chatbot architectures.

Reimers and Gurevych (2019) advanced the field further with Sentence-BERT (SBERT), which utilized a Siamese network structure to create meaningful sentence-level embeddings. This drastically reduced computational overhead for semantic similarity tasks, making it possible to compare thousands of sentences in milliseconds.

The foundation for these innovations was laid by Vaswani et al. (2017), whose Transformer architecture revolutionized text generation and became the backbone of modern large language models. Carlini et al. (2021) later raised critical concerns about these models, showing how training data could be extracted from LLMs, thereby exposing privacy risks.

Jurafsky and Martin (2023) provided a comprehensive overview of speech and language processing, contextualizing the evolution of NLP from rule-based systems to deep learning. Chen et al. (2020) emphasized the role of deep learning in dialogue systems, illustrating how neural architectures improved conversational fluency.